IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA	)	
	)	
v.	)	**Case No. 2:13-cr-00243-001**
	)	
SEAN TIERNAN	)	
	)	

DEFENDANT'S OBJECTIONS TO PRESENTENCE INVESTIGATION REPORT

Five years ago when the FBI raided Sean Tiernan's student housing at Cal Poly and seized his computer, agents believed that the way Sean was making money to fund his college education – using exploits spread via social media to access IP addresses and then selling that access to an individual who sent out harmless spam advertising – negatively impacted the computers affected and invaded the privacy of their owners. The term "malware" was used back then by the government to describe all web-spread exploits, and the presumption was that they were harmful as well as invasive to personal privacy. Fast-forward to the present, and the FBI is now using those same types of exploits to access IP Addresses. In connection with using these exploit tools, FBI agents have testified that exploits of this type – namely those that execute software instructions in the target computer that cause it to transmit its IP Address back -- do no harm to the affected computers. Further, in pleadings in these recent cases, the government has taken the position that individuals do not have a privacy interest in their IP addresses. Consequently, the current technological and legal view is that there is neither physical harm to the affected computer nor a breach of the user's right to privacy when an exploit is deployed over the internet to trigger access to and transmission of an IP address on a private computer.

The Presentence Investigation Report ("PSR") in this case, however, does not reflect this current more sophisticated understanding of the technology and rights involved. Instead, it uses outdated pejorative vocabulary to describe Sean's conduct, thereby significantly overstating the seriousness of the offense and ignores the latest evidence that no harm was done, and consequently it overstates the seriousness of the offense and fails to acknowledge that no loss was caused. It also makes the related error of attributing an actual loss for purposes of adding an enhancement attributable to loss to the sentencing guidelines calculations, and failing to correct more minor errors of fact.

Objection #1: The Description of the Offense Uses Imprecise Outdated Language that Overstates the Seriousness of the Defendant's Conduct

"For last year's words belong to last year's language

And next year's words await another voice."

— T.S. Eliot, Four Quartets

Paragraphs 10-15 of the Presentence Report (PSR), which describe the offense conduct, contains an outdated description of Mr. Tiernan's conduct that makes his crime appear more serious than it was. Using words such as "malware," "infection," "compromised," and "hacked," the PSR describes Mr. Tiernan's activities and implies harm was caused.1 Unlike the traditional criminal case, where the facts once plead are immutable, in the realm of cybercrimes – where using words to describe very sophisticated and evolving technology is a challenge, and definitions evolve along with

1 The use of the term "malware" is outdated and insufficiently precise as it encompasses a wide variety of computer programs vastly more disruptive than then programing engaged in by the defendant. *See https://en.wikipedia.org/wiki/Malware* (defining Malware as an "umbrella" term used to refer to software of vastly different types and that can include legal and illegal applications.).

technology – the description of the offense should reflect the current understanding of the crime, not an outdated one.

Language matters; and the words chosen to describe offense conduct in a criminal case are particularly important because they can be used to determine any number of things including conditions of incarceration and length of sentence. Use of the term "malware" is seriously outdated and insufficiently precise as it encompasses a wide variety of computer programs vastly more disruptive than the programming exploit propounded by Mr. Tiernan. Indeed, at least one federal district court has acknowledged that the word "malware" has "negative connotations. *United States v. Matsh, (*EDVA) 16 CR 16 (6/23/16 Op. Order) Dkt. 90 ("Matsh Order") at 19. Further, by analogizing the exploits to an "infection" and using words such as "compromised," the PSR wrongly created the impression that the computers to which this exploit was applied no longer worked, were slower or "sick" in some way. That is far from the case, and the government has not proffered any evidence to support that view. Overall the description of the offense obscures the essential fact that defendant's software exploit **only** accessed and transmitted the IP Address – which courts now routinely hold is not private -- and identify a port for each device to facilitate sending spam. As such, it did not and could not access protected information on private computers such as bank or financial information. Further, in the normal course of a user's operation of their computer, it was generally removed in fairly short order via the host computer's anti-virus software as that software was updated, consequently the "instructions" the defendant caused to be transmitted into the impacted computer was short-lived. Finally, the defendant only sold access to the IP Address/port information to one purchaser with whom he had a long-standing relationship, and whom he trusted.

Pejorative words are not needed to describe the acts that constitute the offense. The following is how the government described an exploit like the one Sean deployed:

> In the normal course of operation, websites send content to visitors. A user's computer downloads that content and uses it to display web pages on the user's computer. Under the [relevant exploit], the TARGET WEBSITE. . . augment that content with additional computer instructions. When a user's computer successfully downloads those instructions from the TARGET WEBSITE . . . the instructions, which compromise the [exploit], are designed to cause the user's "activating" computer to transmit certain information [including IP Address]. . . . The [exploit] will not deny the user of the "activating" computer access to any data or functionality of the user's computer.

United States v. Matish, EDVA, 16CR16, ECF 24-1 ¶ 33. This neutral language more properly explains what Sean did than the outdated terminology of the PSR. Defendant proposed alternate language of its own that likewise captured the true nature of his actions without the negative and pejorative connotations contained in the PSR's description of the offense. This language is reproduced as Attachment A. As discussed further in relation to Objection #2, no actual harm or loss was caused by defendant's activities.

Objection #2: Defendant's conduct caused no actual loss

When the defendant entered his plea, he admitted that his exploit caused a loss. That admission, however, was predicated on the then-prevalent view that harm was *necessarily* caused when an exploit was deployed to an unsuspecting user's computer to access an IP address. Put another way, it was believed then that the computer's owner had a right to have their computer kept free of unauthorized exploits and a privacy interest in their IP Address. The difficulty measuring that purported actual loss lead the parties here to agree upon an alternate valuation, namely the defendant's profit.

Since the entry of the plea agreement in 2013, however, public expectations have shifted dramatically. As one court explained last year, "society's view of the Internet – and our corresponding expectation of privacy not only in the information we post online but also in our physical computers and the data they contain – recently has undergone a drastic shift." *Matish Order* at 50. People recognize that their computers likely will not be unaffected by use of the Internet, *id.,* and generally understand that their computers can be exposed to innocuous cookies and other injections of software whenever they access a website over the internet. Likewise, courts have come to recognize (almost uniformly) that individuals do not have a privacy right in the IP Addresses of their computers. *Id.* at 43-47 (discussing and collecting cases). Consequently, the presumption that any individual has an expectation – much less a right – to have their computer free from all unauthorized exploits, regardless of how banal, no longer exists.

Indeed, the exploit that defendant designed is remarkably similar to the exploit used by the FBI in the recent Playpen investigation. In that investigation, the government applied for and obtained a search warrant to utilize and deploy a software exploit like that designed by the defendant here. The government calls its exploits Network Investigative Tools or NITs for short. In applying to obtain the search warrant to deploy exploits to gain access to and obtain IP Addresses of users' computers via their NIT, the FBI agent who signed the affidavit did not suggest that the NIT exploit would be harmful in any way to the end users' computers. The Affiant stated, "the NIT does not deny the users or administrators access to the TARGET WEBSITE or the possession or use of the information delivered to the computer controlled by or known to the government, nor does the NIT permanently alter any software or programs on the user's computer." Playpen Affidavit ¶ 41

(*Matish,* ECF # 24-1). He also stated that the exploit "will not deny the user of the 'activating' computer access to any data or functionality of the user's computer." *Id.* ¶ 33. At a subsequent hearing in the *Matish* case, that same FBI agent testified that the exploit, which was used to access and obtain IP Addresses, "did not install any software, it could not remotely take control of the computer, there was nothing left behind. No settings on the computer were altered." *United States v. Matish*, 16 CR 16 (EDVA), ECF # 86 (6/16/16 Tr. at 19-20). This same FBI agent also explained how the exploit worked as follows:

> Q: And I believe you used the analogy that this exploit is like a way of picking a lock, right?
>
> A: Yes. A more accurate analogy may be going in through an open window. As I've stated in my declaration, there was a vulnerability on [defendant's] computer. The FBI did not create that vulnerability. That vulnerability can be thought of as an open window. So we went in through that open window, the NIT collected evidence, and then left. We made no change to the window.

Id. at 33.

In light of these developments – namely the recognition that individuals have no expectation of "clean" computers or in the privacy of their IP Addresses, and the FBI's acknowledgement that exploits of a type similar to defendants cause no harm – the loss in this case should be zero. Defendant consequently objects to the 6 level increase in the offense level on the grounds that the loss was more than $40,000.

The fact that Mr. Tiernan previously agreed to use the amount of his gain to represent the loss in this case should not be held against him, now that law enforcement has come to the realization that exploits are not necessarily harmful. Further, the government has presented no evidence of actual loss and no victim impact statement has been submitted.

Miscellaneous Additional Objections

(a) Page 3: Identifying Data

His place of Birth should be revised to "Hinsdale, IL."

(b) Paragraph 53:

It is our positon that defendant's participation in Alcoholics Anonymous constitutes "formal drug and alcohol treatment" and thus the statement that he reported no history of formal drug and alcohol treatment is inaccurate. Further, the PSR should include the frequency of attendance at AA, which sometimes was daily.

(c) Paragraph 58 :

It is our position that the work that he performed assisting the law enforcement --approximately 40 hours/week in 2012-14 and less thereafter – should be reflected here. His work assisting the FBI, although uncompensated, is equivalent to other types of uncompensated employment, such as internships, and involved an unusually demanding and prolonged time commitment.

(d) Paragraph 59:

The phrase "under the table" in the first sentence is unsupported and inaccurate.

CONCLUSION

For the aforementioned reasons, the PSR should be revised as described herein, and the defendant sentenced accordingly.

Respectfully submitted,

/s/ Carolyn McNiven
Carolyn F. McNiven (IL 6216537; CA 163639)
Greenberg Traurig LLP
4 Embarcadero Center, Suite 3000
San Francisco, CA 94111
Tel: (415) 655-1270
Fax: (415) 520-0855
mcnivenc@gtlaw.com
Lead Attorney
Admitted *Pro Hac Vice*

Attachment A (Proposed Alternate Language)

Paragraphs 10-15 (description of the offense)

Defendant was charged with facilitating the sending via the internet of large amounts of unsolicited commercial emails (a.k.a. "spam") in violation of 18 U.S.C. 1037(a)(1), (b)(2)(A), and 2. He committed this offense by creating computer programs to access and capture the unique IP address and port for private computers owned by private citizens, and then selling access to this information to a single customer with whom he had a longstanding relationship. This customer, in turn, sent spam to these private computers via the internet. Defendant's software programs **only** transmitted the IP Address and a port for each device to facilitate sending spam; and it did not and could not access protected information on private computers such as bank or financial information. Defendant only sold access to the IP Address/port information to one purchaser with whom he had a long-standing relationship. Defendant began this activity as a juvenile when he was living with his parents in Illinois. He continued this activity during the period of the charged conduct, namely August 2011 to October 2012, while attending college in California.

The defendant's computer programs spread from one computer to another via computer users' use of social networking websites. The defendants' programs used a method sometimes referred to as "command and control" (C&C) infrastructure and included the use of compromised servers to assist with routing the software to private computers. Once the defendant's computer code entered the private computer, it automatically communicated back through controlled servers their individual IP addresses and port. The interlinking system of individual computers and compromised servers is sometimes called a "botnet," and the individual computers are sometimes referred to as "bots," which is slang for "robot."

The customer purchased access to the defendant's botnets for a few hundred dollars per week. This customer in turn had the ability to send spam to these "bots" for as long as the defendant's program was active on them. Defendant's programs were routinely removed from the private computers – and thus their function as bots terminated – when installed anti-virus software updated and removed the defendant's program.

At the time of the search of Tiernan's residence and computer via a search warrant on or about October 1, 2012, over 77,000 bots were active in Tiernan's botnet.

At least one of the computers that received spam as a result of this conduct resided in this district.

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that a true and correct copy of the foregoing was e-filed using the CM/ECF this 16th day of June 2017 and served on all appropriate parties through that system.

/s/ Carolyn McNiven
Carolyn F. McNiven
Greenberg Traurig LLP
4 Embarcadero Center, Suite 3000
San Francisco, CA 94111
Tel: (415) 655-1270
Fax: (415) 379-6668
Admitted *Pro Hac Vice*